WHAT IS CLAIMED IS:

1. A system for detecting, tracking and blocking one or more denial of service attacks over a computer network, the system comprising:

a collector adapted to receive a plurality of data statistics from the computer network and to process the plurality of data statistics to detect one or more data packet flow anomalies and to generate a signal representing the one or more data packet flow anomalies; and

a controller coupled to the collector to receive the signal;

wherein the controller is constructed and arranged to respond to the signal by tracking attributes related to the one or more data packet flow anomalies to at least one source, and wherein the controller is constructed and arranged to block the one or more data packet flow anomalies.

2. The system of claim 1, wherein the collector includes a buffer coupled to the computer network and being adapted to process the plurality of data statistics to generate at least one record.

3. The system of claim 2, wherein the collector further includes a profiler coupled to the buffer and being adapted to receive and process the record to generate a predetermined threshold.

4. The system of claim 3, wherein the profiler includes means for aggregating the data statistics to obtain a traffic profile of network flows.

5. The system of claim 4, wherein the data statistics are aggregated based on at least one invariant feature of the network flows.

6. The system of claim 4, wherein data statistics are aggregated based on temporal, static network and dynamic routing parameters.

7. The system of claim 5, wherein the at least one invariant feature includes source and destination endpoints.

8. The system of claim 3, wherein the collector further includes a detector coupled to the buffer and to the profiler, the collector being adapted to receive and process the record and the predetermined threshold to detect if attributes associated with the record exceed the predetermined threshold representing the one or more data packet flow anomalies.

9. The system of claim 8, wherein the collector further includes a local controller coupled to the detector and to the profiler and being adapted to receive and respond to the one or more data packet flow anomalies by generating the signal representing the one or more data packet flow anomalies.

10. The system of claim 9, wherein the detector includes a database for storing the at least one record, predetermined threshold, the one or more data packet flow anomalies, and related information.

11. The system of claim 10, wherein the profiler includes a database for storing a plurality of data packet flow profiles and related information.

12. The system of claim 1, wherein the controller includes a filtering mechanism for blocking the one or more data packet flow anomalies.

13. The system of claim 12, wherein the filtering mechanism includes a plurality of filter list entries.

14. The system of claim 12, wherein the filtering mechanism includes a plurality of rate limiting entries.

15. The system of claim 1, wherein the controller includes a correlator coupled to the collector and being adapted to receive and normalize the plurality of signals representing the one or more data packet flow anomalies and to generate an anomaly table including the attributes related to the one or more data packet flow anomalies.

16. The system of claim 15, wherein the correlator includes a database for storing the anomaly table.

17. The system of claim 16, wherein the correlator further includes an adapter that is constructed and arranged to communicate the anomaly table to a computing device for further processing.

18. The system of claim 16, wherein the controller further includes:

a web server; and

access scripts that cooperate with the web server to enable the computing device to access the database defined on the controller to view the anomaly table.

19. A system comprising:

at least one routing system;

a plurality of computer systems coupled to the routing system; and

means for detecting one or more denial of service attacks communicated to the plurality of computer systems over the at least one routing system.

20. The system of claim 19, further including a means for tracking the one or more denial of service attacks communicated to the plurality of computer systems over the at least one routing system.

21. The system of claim 20, further including a means for blocking the one or more denial of service attacks communicated to the plurality of computer systems over the at least one routing system.

22. The system of claim 21, wherein the means for detecting includes a means for collecting a plurality of data statistics from the at least one routing system.

23. The system of claim 22, wherein the means for detecting further includes a means for processing the plurality of data statistics to detect one or more data packet flow anomalies.

24. The system of claim 23, wherein the means for detecting further includes a means of generating a plurality of signals representing the one or more data packet flow anomalies.

25. The system of claim 24, wherein the means for tracking includes a means for receiving and responding to the plurality of signals by tracking attributes related to the one or more data packet flow anomalies to at least one source.

26. The system of claim 19, further including a means for communicating the one or more denial of service attacks to a computing device for further processing.

27. A method for detecting, tracking and blocking one or more denial of service attacks over a computer network, the system comprising the steps of:

collecting a plurality of data statistics from the computer network;

processing the plurality of data statistics to detect one or more data packet flow anomalies;

generating a plurality of signals representing the one or more data packet flow anomalies; and

receiving and responding to the plurality of signals by tracking attributes related to the one or more data packet flow anomalies to at least one source.

28. The method of claim 27, further including the step of blocking the one or more data packet flow anomalies in close proximity to the at least one source.

29. The method of claim 28, wherein the step of collecting the plurality of data statistics includes:

buffering the plurality of data statistics;

processing the plurality of data statistics to generate at least one record; and

receiving and profiling the at least one record to generate a predetermined threshold.

30. The method of claim 29, wherein the step of collecting the plurality of data statistics further includes;

detecting if attributes related to the at least one record exceed the predetermined threshold representing the one or more data packet flow anomalies.

31. The method of claim 30, wherein the step of collecting the plurality of data statistics further includes:

responding locally to the one or more data packet flow anomalies by generating the plurality of signals representing the one or more data packet flow anomalies.

32. The method of claim 27, wherein the step of receiving and responding to the plurality of signals includes:

correlating the plurality of signals representing the one or more data packet flow anomalies; and

generating an anomaly table including the attributes related to the one or more data packet flow anomalies.

33. The method of claim 32, wherein the step of receiving and responding to the plurality of signals further includes the step of communicating the anomaly table to a computing device for further processing.